CLAIMS

1. A system that is operable to insure authorized access to secured repositories of data and programs, to support protected mutually exclusive execution of programs, comprising:

a first component operable to provide authorized access to said secured repositories of data and programs, to prevent one application from utilizing, scrutinizing or modifying another application,

a second component operable to execute programs loaded from or residing in said repositories of programs and accessing said repositories of data,

said first and second components operating in parallel.

2. The system of claim 1, containing a coordination medium, said coordination medium being operable to conveying information between a plurality of sub-modules within said system, and being operated in compliance with a security rule whereby said coordination medium is detached from the control of any program loaded from or residing in said repositories of programs whenever said coordination medium is attached to said data repositories.

3. The system of claim 1, wherein said repositories of programs are operable to fetch for execution portions of a complete program during program run time.

4. According to claim 3, wherein fetching of portions of a program are subject to a mask controlled by said first component, said mask being a plurality of control values determining which parts of said repositories of programs are operable in an application session.

5. A method of insuring authorized access to secured repositories of data and programs, of to support protected mutually exclusive execution of programs, comprising:

a first process providing authorized access to said secured repositories of data and programs, preventing one application from utilizing, scrutinizing or modifying another application,

a second process of executing programs loaded from or residing in said repositories of programs and accessing said repositories of data,

said first and second processes being performed in parallel.

6. The system of claim 1, operable in a mobile communication device.

7. The system of claim 1, implemented on a single monolithic microelectronic circuit.

8. The system of claim 1, wherein traffic of information between parts of the system that do not reside on a common monolitic microelectronic integrated circuit.

9. The system of claim 1, containing an apparatus for personal identification.

10. The method of claim 5 wherein said controlling of access to secured repositories of data and programs is based on public key encryption.

11. The method of claim 5 wherein said authorized downloading of executable programs is based on public key encryption.

12. A method according to claim 5, wherein applications are exclusively authorized by a certified authority identifiable to the TCE SAM, whereby such authority's public key is immutably programmed into the TCE SAM's non-volatile memory, wherein confidential client programs are licensed to be programmed into, updated and improved after verifiable certification of said authority.

13. A method according to claim 5 wherein a plurality of authorities are licensed to program applications into the TCE SAM's non-volatile memory.

14. A method according to claim 1, wherein at least one analog input to the application environment is operative to input analog data.

15. A method according to claim 5, wherein at least one analog input to the application environment is operative to input analog data.

16. A method according to claim 14 wherein said input data corresponds to an image.

17. A method according to claim 15 wherein said input data corresponds to an image.

18. A method according to claim 1, wherein said image is derived from the output of a fingerprint detector operative to provide data for feature extraction typically to prepare a feature matrix to identify the possessor of said fingerprint.

19. A method according to claim 5, wherein said image is derived from the output of a fingerprint detector operative to provide data for feature extraction typically to prepare a feature matrix to identify the possessor of said fingerprint.

20. A method according to claim 1, wherein said sensed feature matrix is compared to at least one trained matrix residing in the secured memory repository.

21. A method according to claim 5, wherein said sensed feature matrix is compared to at least one trained matrix residing in the secured memory repository.

22. A method according to claim 1, wherein the analog data corresponds to a voice message.

23. A method according to claims 5, wherein the analog data corresponds to a voice message.

24. A method according to claim 22, wherein features are extracted from the voice message operable to identify the speaker

25. A method according to claim 23, wherein features are extracted from the voice message operable to identify the speaker

26. A method according to claim 1, wherein previous to initializing an application session no application data pertaining to a previous application session remains in the application environment partition.

27. A method according to claim 5, wherein previous to initializing an application session no application data pertaining to a previous application session remains in the application environment partition.

28. A method according to claim 1, wherein following an application session, executable memory and data memory are all reset.

29. A method according to claim 5, wherein following an application session, executable memory and data memory are all reset.

30. A method according to claim 1, wherein the circuits are embedded in smart cards.

31. A method according to claims 5, wherein the circuits are embedded in smart cards.

32. A method according to claim 1 wherein the circuits are embedded in the subscriber identification modules of mobile communication devices.

33. A method according to claim 5 wherein the circuits are embedded in the subscriber identification modules of mobile communication devices.

34. A method according to claim 1 wherein the circuits are operable to enhance security and functionality in computer network servers.

35. A method according to claim 5 wherein the circuits are operable to enhance security and functionality in computer network servers.

36. A method according to claim 1 wherein the circuits are operable to enhance security and functionality of mass storage devices.

37. A method according to claim 5 wherein the circuits are operable to enhance security and functionality of mass storage devices.

38. A method according to claims 1 wherein the circuits are operable to enhance security and functionality of computing devices.

39. A method according to claims 1 wherein the circuits are operable to enhance security and functionality of computing devices.

40. A method according to claim 1 wherein the system can authenticate the validity and integrity of multi-origin data files

41. A method according to claim 5 wherein the system can authenticate the validity and integrity of multi-origin data files

42. A method according to claim 14, wherein visual data, input in clear text to the application computing environment is synchronized with audio data which is decompressed in the device wherein both media are output simultaneously in separate streams to the display device.

43. A method according to claim 15, wherein visual data, input in clear text to the application computing environment is synchronized with audio data which is decompressed in the device wherein both media are output simultaneously in separate streams to the display device.

44. A method according to claim 16, wherein fine tuning portions of visual data residing in the data repository are intertwined with the audio data of the SAM and are typically operative to enhance the visual data input in the clear from the host, to thereby typically prevent quality duplication of the digitized visual data.

45. A method according to claim 17, wherein fine tuning portions of visual data residing in the data repository are intertwined with the audio data of the SAM and are typically operative to enhance the visual data input in the clear from the host, to thereby typically prevent quality duplication of the digitized visual data.

46. The system of claim 1, imbedded within a wireless communication device.

47. The system of claim 1, serving a credit or debit charge card clearance scheme.

48. The system of claim 1, operative to display flight schedule, to reserve flights, to ticket flights, and to clear payments for airline services.